REMARKS

Claims 1-2, 4-20, 31, 38-41, and 43-48 are pending in the application.

The examiner rejected independent claims 1, 38, and 47 under 35 U.S.C. §103(a) as being unpatentable over Jones in view of ElGamal. The examiner admits that Jones does not disclose:

> [a] protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret or the third secret

as recited in claims 1, 38, and 47, and relies on ElGamal to supply this feature. The examiner argues that:

> Elgamal discloses a key distribution scheme wherein the party A and B compute the secret K_{AB}… The party A has a secret x_A and B has a secret x_B. The party A, which corresponds to the client, obtains the third secret (K_{AB}). The party A has a secret x_A and B has a secret x_B, therefore the party A cannot determine the secret of Party B and Party B cannot determine the secret of Party A (Office Action, p. 3).

However, even if we assume that party A is the client with client secret x_A, party B is the server with server secret x_B, and K_{AB} is the third secret, and even if parties A and B cannot determine each other's secrets, ElGamal's scheme is missing an important element of the claim. Specifically, ElGamal does not teach or suggest a protocol in which the server, i.e., party B, cannot feasibly determine the third secret, i.e., K_{AB}, as required by the claim.

In fact, ElGamal discloses exactly the opposite of what is required by the present claims. More specifically, <u>both party A and party B need to know K_{AB}</u>. According to ElGamal:

> Suppose that <u>*A* and *B* want to share a secret K_{AB}</u>… *A* computes $y_A=\alpha^{xA}$ mod p, and sends y_A. Similarly, *B* computes $y_B=\alpha^{xB}$ mod p and sends y_B. Then the secret K_{AB} is computed as
>
> $$K_{AB} \equiv \alpha^{xA} \bmod p$$
> $$\equiv y_A^{xB} \bmod p$$
> $$\equiv y_B^{xA} \bmod p$$
>
> Hence, <u>both</u> *A* and *B* are able to compute K_{AB} (p. 469, emphasis added).

After computing K_{AB}, parties A and B securely communicate with each other by encrypting messages using K_{AB} and decrypting the encrypted messages with x_A and x_B. ElGamal provides

an example of how to do this: party A selects a random value k, which is equivalent to x_A; calculates K, which is equivalent to K_{AB}; and encrypts message m under K by computing $c_1 \equiv \alpha^k$ mod p and c_2=Km mod p. Then, party A sends c_1 and c_2 to party B (p. 469). Party B recovers message m by first recovering K, and then using K to decrypt m:

> The decryption operation splits into two parts. The first step is recovering K, which is easy for B since K $K_{AB} \equiv (\alpha^k)^{xB} \equiv c_1^{xB}$ mod p, and x_B is known to B only. The second step is to divide c_2 by K and recover the message m (p. 469).

So, party B recovers K so that it can decrypt message m. Therefore party B knows K.

In order for ElGamal's scheme to work, both A and B must know K. But if one equates party B with the claimed "server," and K (which is equivalent to K_{AB}) with the claimed "third secret," ElGamal explicitly teaches away from a protocol wherein the "server cannot feasibly determine the client secret or the third secret," as is required by claims 1, 38, and 47, and claims dependent thereon.

For at least the reasons stated above, applicant believes the pending application is in condition for allowance, and asks the examiner to allow the claims to issue.

A request for a three-month extension of time accompanies this response. Please charge the extension fee for this request to Deposit Account No. 08-0219. Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,

Dated: July 28, 2006

Eric L. Prahl
Registration No.: 32,590
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(6170 526-6043 (telephone)
(617) 526-5000 (facsimile)